Ausschreibungsunterlage

Leistungsbeschreibung

Beschaffung und Einführung einer Mobile-Device-Management-Lösung (On-Premise)

Vivantes Netzwerk für Gesundheit GmbH

1. Einleitung und Zweck der Ausschreibung

Die Vivantes Netzwerk für Gesundheit GmbH beabsichtigt, eine aktuelle Mobile-Device-Management-Lösung (MDM) für den unternehmensweiten Einsatz neu auszuschreiben. Die Lösung soll den Betrieb von aktuell rund 5.000 mobilen Endgeräten (Smartphones, Tablets) zentral verwalten, absichern und kontrollieren.

Als Betreiber einer kritischen Infrastruktur (KRITIS) im Gesundheitswesen unterliegt das Unternehmen höchsten Anforderungen an die Informationssicherheit, Ausfallsicherheit, Resilienz und Integrität der IT-Systeme gemäß NIS2 und BSIG. Entsprechend streng sind die Sicherheits-, Compliance- und Qualitätsstandards für die einzusetzende Software.

Diese Leistungsbeschreibung definiert den funktionalen Leistungsgegenstand. Einzelheiten zu den funktionalen und technischen Anforderungen sind dem Anforderungskatalog zu entnehmen.

2. Beschreibung des Ist-Zustandes

- **Systemumgebung**: Die aktuelle On-Premise-MDM-Umgebung basiert auf Ivanti Endpoint Manager Mobile (EPMM).
- **Bestandteile des aktuellen Systems**: Die bestehende Umgebung umfasst 99 Konfigurationen, 35 Policies und 90 verwaltete Applikationen.
- **Schnittstelle**: Aktuell wird eine REST-API-Schnittstelle eingesetzt, über die unser internes ESM-System die Verbindung zum System herstellt.
- **Geräte**: Es werden aktuell rund 5.000 mobile Endgeräte (aktuelle Verteilung 95% iOS und 5% Android) verwaltet.
- **Infrastruktur**: Der Betrieb erfolgt im eigenen Rechenzentrum der Vivantes Netzwerk für Gesundheit GmbH in Berlin.

3. Gegenstand der Leistung (Soll-Zustand)

- Lieferung, Lizensierung und Installation der Software in der IT-Infrastruktur des Auftraggebers (On-Premise) gemäß der funktionalen und technischen Anforderungen des Anforderungskatalogs
- Einrichtung und Konfiguration gemäß den betrieblichen Anforderungen des Auftraggebers
- Migration der bestehenden der bestehenden Geräte-, Profil- und Richtlinienbestände aus der aktuellen MDM-Umgebung
- Schulung der administrierenden Mitarbeitenden
- **Hardware:** Es wird *keine* Hardware (Endgeräte oder physische Server) beschafft; die Ausschreibung bezieht sich rein auf Softwarelizenzen, Implementierung und Support.

- **Lizenzmodell:** Der Auftragnehmer hat Lizenzen für die Verwaltung, Kontrolle und Absicherung von bis zu 5.000 Geräten bereitzustellen. Zulässig ist sowohl ein Kaufmodell als auch ein Subskriptionsmodell bezogen auf einzelne Gerätelizenzen als auch die Bereitstellung einer Campuslizenz – ebenfalls zum Kauf oder im Subskriptionsmodell.

  Im Falle einer Campuslizenz ist eine uneingeschränkte Nutzung der Mobile-Device-Management-Lösung (On-Premise) zu gewährleisten. Die Lizenz muss die Anmeldung und Verwaltung von bis zu 5.000 Endgeräten des Auftraggebers sowie eine entsprechende Anzahl von Geräte-Installationen abdecken, ohne dass zusätzliche geräte- oder mengenbezogene Lizenzgebühren anfallen. Optional muss die Campus-Lizenz die Verwaltung von weiteren bis zu 5.000 Endgeräten, d.h. insgesamt maximal 10.000 Endgeräte, ermöglichen. Der Auftraggeber kann diese Option im Bedarfsfall durch einseitige Erklärung abrufen.

  Falls Gerätelizenzen auftragsgegenständlich sind, hat der Auftragnehmer eine Option für die Erweiterung des Gerätebestandes angeboten, die der Auftraggeber im Bedarfsfall durch einseitige Erklärung abrufen kann. Durch die Ausübung der Option kann der Auftraggeber während der Vertragslaufzeit zu jedem Zeitpunkt zusätzliche Lizenzen in einer flexiblen Mengenstaffelung hinzubuchen. Die maximal abzudeckende Geräteanzahl ist auf 10.000 begrenzt.

  Dem Subskriptionsmodell ist ein initialer Vertragszeitraum von drei Jahren zugrunde zu legen, der nach Bedarf des Auftraggebers optional um jeweils ein Jahr verlängert werden kann. Der Auftragnehmer unterstützt den Auftraggeber im Subskriptionsmodell vor dem Ende des Vertragszeitraum soweit erforderlich bei der Vorbereitung der zukünftigen Migration der MDM-Lösung in die Nachfolgelösung (Exit-Management).

  Welches der vorstehenden Modelle vertragsgegenständlich wird, richtet sich danach, auf welches Angebot der Zuschlag erteilt wurde.

3.1 Implementierung, Migration und Rollout

- **Implementierung:** Der AN konfiguriert und implementiert zudem die Cluster-Fähigkeit des Systems, die Integration in das Active Directory (LDAPS) sowie die Anbindung an das SIEM.

  Alle notwendigen Voraussetzungen zur Installation in einer On-Premise-Umgebung werden vom AG zur Verfügung gestellt (notwendige virtuelle Server, Firewalleinstellungen). Der Auftraggeber stellt eine Remoteverbindung zur Installation der Software bereit. Die Implementierungs- und Migrationsleistungen können vor Ort beim Auftraggeber oder Remote erbracht werden.

- **Migration:** Der Auftragnehmer erbringt die Migrationsleistungen auf Grundlage des von ihm mit dem Angebot einzureichenden Migrationskonzepts, welches die Übernahme der bestehenden Geräte-, Profil-, Richtlinien- und Applikationsbestände aus der Ivanti-Umgebung in das neue MDM-System regelt. Das Migrationsvorgehen muss darauf ausgelegt sein, Betriebsunterbrechungen zu minimieren.

  Die zu migrierende Konfiguration des AG umfasst derzeit 99 Configurations, 35 Policies und 90 verwaltete Applikationen.

  Bei den 99 Configurations handelt es sich insbesondere um WLAN, Exchange, App Restrictions, Managed App Configs, die Konfiguration des Inhouse-Appstores, Zertifikate, VPN, Restrictions, Webclips und Web-Content-Filter. Die 35 Policies umfassen insbesondere

Homescreen-Layouts, Lockscreen-Messages sowie Security- und Sync-Einstellungen. Die 90 verwalteten Applikationen werden aktuell über die Ivanti-Umgebung verteilt und setzen sich aus Apps des Volume Purchase Program (VPP) und Inhouse-Apps des AG zusammen.

Die Migration des AN umfasst die Überführung aller genannten Bestände einschließlich der zugehörigen Zuweisungen und Konfigurationen sowie der Lizenzen der VPP-Apps und der Inhouse-Apps samt Anbindung an den Inhouse-Appstore in das neue MDM-System.

Die Migration erfolgt vor der eigentlichen Umstellung der Nutzer, sodass die Konfigurationen und Applikationen zum Zeitpunkt des Rollouts vollständig im neuen System bereitstehen und geprüft sind.

Der AG ist bei der Vorbereitung und Durchführung der Migration umfassend einzubeziehen. Der AN hat daher sicherzustellen:

- die Anwesenheit des AG während der Durchführung der Migration
- die Organisation und Planung der Migrationstermine in Abstimmung mit dem AG durch den AN

- **Rollout:** Der AN unterstützt den AG bei der Umstellung der Endgeräte durch die Nutzer in Wellen. Der AN übernimmt das Monitoring und unterstützt den AG bei Problemen.

3.2 Schulung

Schulung von 5-10 Systemadministratoren (2nd/3rd Level) in der Systemkonfiguration und im Troubleshooting sowie Bereitstellung digitaler Schulungsunterlagen/Handbücher in deutscher Sprache.

3.3. Support und Wartung

Deutschsprachiger Support mit Servicezeiten von Montag bis Freitag in den Zeiten von 08:00 bis 17:00 Uhr und den folgenden Mindest-Vorgaben (die Reaktions- und Wiederherstellungszeiten beginnen und laufen nur innerhalb der Servicezeiten):

Art der Störung	**Reaktionszeit in Stunden**	**Wiederherstellungszeit in Stunden**
Betriebsverhindernder Mangel	4	9
Betriebsbehindernder Mangel	24	27
Leichter Mangel	72	126

Die Reaktions- und Wiederherstellungszeiten sind während der gesamten Vertragslaufzeit vertragsstrafenbewehrt. Der Auftraggeber ist für den Fall der Überschreitung der vereinbarten Reaktions- und Wiederherstellungszeiten berechtigt, innerhalb der Servicezeiten für jede angefangene Stunde, die sich der Auftragnehmer mit der Einhaltung der Reaktions- und Wiederherstellungszeiten in Verzug befindet, jeweils eine Vertragsstrafe in Höhe von 0,02 % der Gesamtvergütung für den Systemservice in den ersten drei Vertragsjahren zu verlangen. Insgesamt darf die Summe der zu zahlenden Vertragsstrafen jedoch nicht mehr als 5 % der Gesamtvergütung für den Systemservice in den ersten drei Vertragsjahren betragen.

Bereitstellung eines Ticketsystems für die Störungsmeldungen sowie einer Hotline während der oben genannten Service-Zeiten.

Ergänzend gilt in Bezug auf das Schwachstellenmanagement und die Bereitstellung von Sicherheitsupdates:

- **Monitoring- und Meldepflicht**. Der Auftragnehmer ist verpflichtet, ein kontinuierliches und lückenloses Schwachstellenmonitoring zu gewährleisten. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 24 Stunden, in Textform über jede erkannte Sicherheitsschwachstelle. Die Monitoring- und Meldepflicht gilt unabhängig vom Schweregrad für alle vertragsgegenständlichen Produkte und Leistungen. Sie umfasst auch eingesetzte Komponenten von Drittanbietern und Open-Source-Software.

- **Inhalt der Meldung**. Die Meldung enthält mindestens:

  - eine Beschreibung der Schwachstelle und ihrer möglichen Auswirkungen sowie die betroffenen Produkte und Versionen,
  - die CVE-Kennung (sofern vergeben) und die Bewertung nach CVSS (Version 3.1 oder höher),
  - Informationen über eine bekannte aktive Ausnutzung,
  - verfügbare Sofort- oder Umgehungsmaßnahmen,
  - den geplanten Zeitpunkt für die Bereitstellung eines Sicherheitsupdates.

  Angaben, die zum Zeitpunkt der Meldung noch nicht vorliegen, sind unverzüglich nachzureichen.

- **Frist zur Bereitstellung von Sicherheitsupdates für kritische Schwachstellen**. Für Schwachstellen mit einem CVSS-Basiswert von 9,0 oder höher stellt der Auftragnehmer dem Auftraggeber das Sicherheitsupdate spätestens 24 Stunden nach dessen Veröffentlichung durch den Hersteller bereit. Maßgeblich ist der vom Hersteller oder in der National Vulnerability Database (NVD) veröffentlichte Wert. Weichen die Bewertungen voneinander ab, gilt der höhere Wert.

- **Überbrückung bis zum Update**. Solange für eine kritische Schwachstelle noch kein Sicherheitsupdate verfügbar ist, stellt der Auftragnehmer dem Auftraggeber unverzüglich wirksame Maßnahmen zur Risikominderung zur Verfügung. Er informiert den Auftraggeber fortlaufend über den Stand der Behebung.

- **Vertragsstrafe**. Die Monitoring- und Meldepflichten sowie die Pflicht zur Bereitstellung von Sicherheitsupdates für kritische Schwachstellen sind während der gesamten Vertragslaufzeit vertragsstrafenbewehrt.

  Der Auftraggeber ist für den Fall, dass die Meldung einer Schwachstelle trotz der Kenntnis des Auftragnehmers oder aufgrund der fahrlässigen Unkenntnis des Auftragnehmers von der Schwachstelle unterbleibt, berechtigt, jeweils eine Vertragsstrafe in Höhe von 1,0 % der Gesamtvergütung für den Systemservice in den ersten drei Vertragsjahren zu verlangen.

  Der Auftraggeber ist für den Fall, dass der Auftragnehmer mit der Bereitstellung des Sicherheitsupdates für kritische Schwachstellen in Verzug gerät, berechtigt, jeweils eine Vertragsstrafe in Höhe von 1,0 % der Gesamtvergütung für den Systemservice in den ersten drei Vertragsjahren zu verlangen.

Insgesamt darf die Summe der zu zahlenden Vertragsstrafen jedoch nicht mehr als 5 % der Gesamtvergütung für den Systemservice in den ersten drei Vertragsjahren betragen.

Die Support-Leistungen müssen für drei Jahre erbracht werden und können nach Bedarf des Auftraggebers optional um jeweils ein Jahr verlängert werden.

3.4 Zusatzleistungen (optionale Abrufleistungen)

Bereitstellung eines Kontingents von 10 Personentagen pro Jahr (unverbindliche Schätzung) für künftige Consulting-Leistungen (z.B. bei der Einführung neuer Features), abrufbar nach Bedarf.

3.5 Projektplan

Der Auftragnehmer hat mit dem Angebot einen initialen Projektplan vorgelegt. Die Implementierung der Lösung inklusive des Abschlusses der Migration und dem Go-Live des neuen Systems muss im 1. Quartal 2027 erfolgen.

Der Auftragnehmer führt das Projekt eigenverantwortlich unter Einhaltung der nachfolgenden Meilensteine durch. Die Termine sind als Mindestvorgaben verbindlich und in den Projektplan zu überführen.

Nr.	Meilenstein	Termin
M1	Zuschlagserteilung	T0
M2	Projektstart und Vorbereitung: Kick-off, Abstimmung der Rollen und Ansprechpartner, Klärung der Voraussetzungen (Server, Netzwerk, Zertifikate).	T0 + 5 Werktage
M3	Installation und Integration: Installation des MDM-Systems auf dem Server des AG, Einrichtung der Cluster-Fähigkeit, Integration in das Active Directory (LDAP), Anbindung an das SIEM sowie Einrichtung der Apple-Schnittstellen (z. B. Apple Business Manager, APNs, VPP).	T0 + 5 Wochen
M4	Migration von der Configurations, Policies und verwalteten Applikationen	T0 + 8 Wochen
M5	Übergabe Dokumentation und Durchführung Schulungen	T0 + 10 Wochen
M6	Rollout und Projektabschluss: Umstellung der Endgeräte durch die Nutzer in Wellen, begleitet durch den AN (Monitoring, Unterstützung bei Problemen), anschließend Stabilisierungsphase, Übergabe in den Regelbetrieb und Gesamtabnahme.	T0 + 12 Wochen
M7	Abschluss Parallelbetrieb und Außerbetriebnahme Altsysteme	T0 + 13 Wochen